AUTHENTICATION VIA SMARTPHONE WITH NFC

Matěj Horák

High School Student (3), Bishop Grammar School Žďár nad Sázavou

E-mail: horak.matej.zdar@gmail.com

Supervised by: Lukáš Malina

E-mail: malina@feec.vutbr.cz

Abstract: This work is about replacement smartphones instead of smart cards in acces control. The main goal is to create an application which runs on Android and has the same function as a smart card. The requirements for this task are Smartphones with NFC (Near Field Communication) and Android KitKat OS version or higher version. The authentication protocol is based on using the hash function. This work shows main parts of the source code. The implementation contains the main service class which is based on the HCE (Host-Based Card Emulation) service, cryptographic methods and a graphic user interface.

Keywords: NFC, Authentication, Android, Smartphone, HCE, Security

1. ÚVOD

Dnes je doba mobilních technologií. Nejen mobilní telefony, ale i chytré hodinky nebo brýle, jsou na vzestupu a stávají se z nich zařízení určená pro mnoho užitečných operací a aplikací. A jednou z těchto operací je autentizace uživatele v přístupových systémech, kde mobilní telefony pomalu začínají nahrazovat běžné čipové karty.

Jsou k tomu využívány telefony se systémem Android verze 4.4 (neboli KitKat) a vyšší, popř. lze využít i platformu iOS, kde byla tato funkce představena teprve nedávno, a které jsou vybaveny technologií NFC. Aplikace, která pak slouží pro obsluhu, provádí emulaci čipové karty (Host-Based Card Emulation).

Budoucí běžnou praxí této služby bude otevření přístupových dveří mobilním telefonem, popř. pla-

cení mobilním telefonem v obchodech vybavenými čtečkami na bezkontaktní kartu.

Tato práce je zaměřena na implementaci této služby na platformu Android. Podrobně vysvětluje komunikaci autentizačního protokolu, uvádí důležité části zdrojového kódu a na závěr se zaměřuje na zkušenosti, které jsem získal během vývoje.

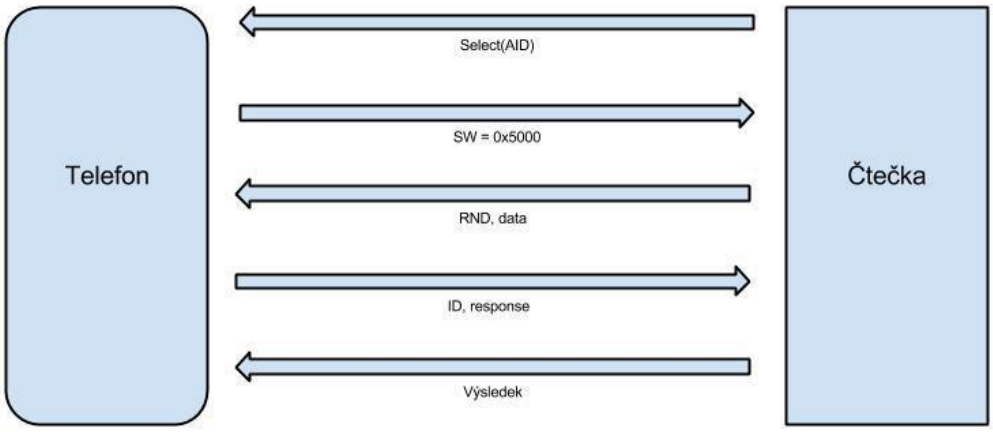
2. POUŽITÝ HARDWARE A SOFTWARE

Na programování aplikace pro platformu Android jsem použil Android Studio verze 1.0.2 na PC se systémem Windows. Pro vývoj pak bylo potřebné také SDK verze 19.

Aplikace byla testována na mobilním telefonu Nexus 5 se systémem Android 5.0.1. Tento telefon je navržen společností Google, která udává směr těchto zařízení. Proto nalezneme na tomto zařízení i technologii NFC. Jako čtecí zařízení jsem použil druhé zařízení Android, které dokáže suplovat dnešní čtečky přístupových systémů, konkrétně telefon Huawei Ascend P7.

3. SCHÉMA KOMUNIKACE AUTENTIZAČNÍHO PROTOKOLU

Jakmile dojde k přiblížení telefonu ke čtečce, dojde k zahájení komunikace. Teoretický dosah NFC technologie se pohybuje okolo 10 cm, v praxi je však nutné zařízení přiblížit na méně než 2 cm. Na obrázku 1 je znázorněn proces, při kterém dochází ke komunikaci mezi telefonem a čtecím zařízením.



Obrázek 1: Schéma komunikace

V prvním kroku čtecí zařízení vyšle tzv. Select (AID), který určuje jakou aplikaci pro obsluhu má zařízení použít. V případě, že zařízení obsahuje dvě a více aplikací se stejným AID (Application Identifier), otevře se na zařízení dialog pro vybrání konkrétní aplikace.

V druhém kroku (už vybraná) aplikace pošle SW = 0x5000, což je tzv. STATUS WORD, který indikuje stav emulované čipové karty. Pro STATUS WORD jsou 3 varianty, které lze poslat. První je

0x9000, která hlásí, že stav je v pořádku. Druhá je 0x6…, která znázorňuje status chyb. Třetí je možnost naprogramovat si SW vlastní, v našem případě 0x5000.

V třetím kroku čtečka pošle RND, neboli náhodné číslo, které je součástí ověření spojení. Je možné připojit i data, která aplikace může potřebovat, např. ID čtecího zařízení.

Čtvrtý krok je nejdůležitější. Mobilní telefon odešle přes spojení ID své karty a response, což je zpráva HMAC, která prošla funkcí HASH (konkrétně SHA-2), a obsahuje RND, přiložená data a K_s, neboli Secret key, který je uložen na obou stranách. Na straně čtecího zařízení se pak vytvoří HMAC zpráva, která se porovná s HMAC zprávou, kterou zařízení přijalo, pokud je stejné jedná se o první ověření, že mobilní telefon je zařízení, které má oprávnění např. otevřít dveře. Druhé ověření je pak samotné ID karty.

V posledním kroku čtecí zařízení odešle výsledek komunikace a dochází k zániku spojení.

Výše popsaný protokol lze nahradit i jinými autentizačními protokoly, které díky velké výpočetní efektivitě mobilního telefonu mohou být založené na asymetrické kryptografii, např. certifikáty.

4. HLAVNÍ ČÁSTI ZDROJOVÉHO KÓDU

Host-Based Card Emulation je služba, proto je nutné implementovat service class. Na obrázku 2 je částečně ukázáno jak tuto service implementovat. Využíváme třídy HostApduService, která už má definované všechny „odchytávače událostí“, které se během komunikace běžně dějí.

```
public class MyHostApduService extends HostApduService
                                {
    @Override
    public byte[] processCommandApdu(byte[] apdu, Bundle extras) {... }
    @Override
    public void onDeactivated(int reason) {... } ...

}
```

Obrázek 2: Ukázka service pro obsluhu emulace

Je potřeba službu uvést v AndroidManifest.xml, kde je potřeba dát pozor na aid-list, který definuje

AID pro tuto aplikaci, viz obrázek 3.

```
<service android:name=".MyHostApduService" android:exported="true"
         android:permission="android.permission.BIND_NFC_SERVICE">
    <intent-filter>
        <action andro-
id:name="android.nfc.cardemulation.action.HOST_APDU_SERVICE"/>
    </intent-filter>
    <meta-data android:name="android.nfc.cardemulation.host_apdu_service"
               android:resource="@xml/apduservice"/>
</service>
```

Obrázek 3: Část Android Manifest

5. VÝSLEDNÁ APLIKACE

Během vývoje výsledné aplikace jsem měl mnoho možností, jak aplikaci naprogramovat (ať už se jednalo o fungování aplikace, nebo vzhled). Zde jsem musel zvážit, zda upřednostnit větší bezpečnost nebo jednoduchost ovládání. Nakonec jsem zvolil druhou variantu, protože stejně jako u čipových karet, je potřeba, aby celý proces byl co nejrychlejší, a proto na ověření hesla, zda se jedná o majitele telefonu, nebyl prostor. Aplikaci jsem také naprogramoval tak, že pro aktivování přenosu NFC stačí mít rozsvícený display a aplikace tak nemusí být vůbec spuštěná. Proto jsem zvolil i jednoduchý design, který se však řídí design guidelines, které jsou k dispozici v oficiální dokumentaci.

6. ZÁVĚR

Během programování této aplikace bylo vyřešeno několik aplikačních i technických problémů, např. implementace funkce HASH nebo nefunkčnost technologie NFC na čtecím zařízení. Použití přímo této aplikace v praxi však nebude, protože spíše simulovala dnešní firemní řešení, jako např. IMA s. r. o.

Tato technologie, která emuluje čipové karty, se již implementuje do praxe a je zřejmé, že za pár let bude běžnou realitou. Toto téma mne velmi zajímá a rád bych se mu věnoval i nadále a nahradil stávající autentizační protokol za protokol, který je založen na asymetrické kryptografii. Rád bych ji využil i v praxi, např. na škole, popř. v jednom bytovém domě. V případě bytového domu by sloužila k odemykání dveří, zatímco na škole, kde se čipové karty používají i na vyzvednutí obědů), by aplikace mohla být rozšířena o modul, přes který by se obědy mohly objednat.

PODĚKOVÁNÍ

Tato práce vznikla během studentské stáže v rámci programu Otevřená věda IV - popularizace výzkumu a vývoje a podpora badatelsky orientované výuky (reg. číslo CZ.1.07/2.3.00/45.0041.). Poděkování také patří mému lektorovi stáže Ing. Lukáši Malinovi Ph. D., který mi byl nápomocen a poskytl mi účinnou metodickou, pedagogickou a odbornou pomoc a další cenné rady při zpracová- ní této práce.

REFERENCE

[1] GOOGLE. API Guides: NFC Basics and Advanced NFC [online]. [cit. 2015-02-24]. Dostupné z: http://developer.android.com/guide/index.html

[2] MATYÁŠ, Vašek a Jan KRHOVJÁK. Autorizace elektronických transakcí a autentizace dat i uživatelů. Brno: Masarykova univerzita, 2008, 125 s. ISBN 9788021045569.